External Penetration Testing

Don't Make it Easy

Attackers are constantly trying to see what they can get into whether they're sitting at home, a coffee shop, or even right outside of your office building. Your external network includes servers and devices visible to the public. If you have even one small vulnerability in your external network, they can easily use it to gain more and more access and potentially compromise your sensitive company information right under your nose.

An External Penetration Test (EPT) can help you get ahead of attackers and determine how vulnerable your systems and external interfaces are before they do. Determine whether your security policies are effective, uncover unknown vulnerabilities, and be able to fix identified vulnerabilities before a data breach occurs. With new threats and vulnerabilities being discovered every day, it is important for your organization to be proactive and get ahead of attackers.

What We've Noticed

The most common vulnerabilities discovered during an EPT are related to network configuration. Many default systems that organizations use to communicate over their networks actually allow malicious attackers to capture information as it travels through the network, leaving your organization vulnerable to a breach. Another common vulnerability comes from your device and service configurations. Leaving default configurations on any device may not seem harmful, but it provides an easy access point for attackers to access sensitive areas.

Know Where You Stand

External Penetration Testing simulates what an attacker could do externally (through firewalls, web servers, mail servers, etc.) if you were targeted. With an EPT, we'll perform a vulnerability scan of your external network and then actually try to exploit any found vulnerabilities them using real-world techniques that attackers are using. Beyond vulnerability scanning, we typically find additional vulnerabilities that may not have been picked up during scanning, like detecting the security of information as it is being transmitted over the network. Once we complete testing, you'll receive a full report with recommendations on how to remediate your vulnerabilities as well as documented evidence of all testing that was performed during the engagement.

External Penetration Testing Features:

- **Determines weaknesses of external security measures**
- **Manual testing of found vulnerabilities**
- **Utilizes tools and techniques used by hackers**
- **Comprehensive report with actionable recommendations for remediation**

Frequently Asked Questions

What is the difference between vulnerability scanning and penetration testing?
Vulnerability Scanning is an automated method that identifies vulnerabilities that may exist on an organization's network. Penetration testing is by nature more accurate than vulnerability scanning since it actually confirms that a suspected weakness is exploitable.

Will this hurt my network?
This is extremely unlikely. We very rarely have any reported problems. We do not attempt any denial of service attacks.

What information does my core provider or IT MSP need to provide during the scoping call?
IP addresses of external interfaces, best times for the automated scans, white-listing process for our IPs, contact information, and domain lockout policy so that we can mitigate the risk of locking out domain users during testing up front.

Are the vulnerability scan results included in the report?
No. If scan results were included, it would be a very long report and there is really no reason to include them. We will often take a screenshot to show the client scans were run and sometimes the specific vulnerability that we were able to exploit.

What is the Information Security Analyst looking for?
We are looking for system and service level vulnerabilities which can potentially be exploited on systems that can be accessed from the public internet. These vulnerabilities could include out-of-date software versions, insecure system configurations, or other technical flaws. The goal is to identify these exploitable vulnerabilities by attempting to compromise these systems using real-world techniques and provide subsequent recommendations on how to mitigate the confirmed attack methods.

What if x hour(s) of testing isn't enough? Do you stop at x hour(s) if you are still finding things?
We do our best to work with you upfront to identify how long testing will take. If after the ISA runs their initial port and networking scans and finds a lot more open ports than expected, or is in the middle of testing and realizes they will need significantly more time, they will contact you.